## Como coletar registros ProcMon para solucionar problemas de AMP na inicialização

## Contents

Introduction Procedimento:

## Introduction

Como administrador de sistema, você pode querer obter registros detalhados usando o Process Monitor (procmon.exe) para determinar se o conector FireAMP trava durante o processo de inicialização do computador. Esses registros também serão solicitados pelo Cisco TAC para solucionar esses problemas. O Process Monitor é um utilitário gratuito que pode nos ajudar aqui. Pode ser baixado gratuitamente em <u>https://docs.microsoft.com/en-us/sysinternals/downloads/procmon</u>

Este documento descreve as etapas sobre como coletar registros ProcMon e despejo de memória se o problema ocorrer durante um processo de inicialização do sistema (o que significa que ele está gerando BSODs na inicialização). Esses registros são necessários para capturar os eventos do sistema que ocorrem durante a inicialização.

## Procedimento:

1. Configurar as máquinas de ensaio de modo a que o problema possa ser facilmente reproduzido.

2. Baixe e execute a ferramenta ProcMon como administrador. Vá para File -> Process Monitor Backing Files e selecione um Path.

cass Monitor - C/(Dani/win7464 naw/Decktop/proce	son_output/sosti_pml				
dit Event Filter Tools Cytlons Help	-				
3 3 8 6 7 4 6 8 8 8 5 8	M A R				
Process Name         PID         Operation         Path           In Sech Indexer         222         Valid System/Correl/C         Sech Indexer         222         Valid System/Correl/C           In Sech Indexer         222         Valid System/Correl/C         Sech Indexer         222         Valid System/Correl/C           In Sech Indexer         2210         Valid System/Correl/C         Sech Indexer         2210         Valid System/Correl/C           Indexer         2210         Valid System/Correl/C         Sech Index North Valid System/Correl/C         Sech Index North Valid System/Correl/C           Indexer         2210         Valid System/Correl/C         Sech Index North Valid Vali	Schware Classes Schware Classes Schware Classes Schware Classes Schware Classes / Mil.	Pand SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS SUCCISS	Detail Cerest FSCTL_G. Cerest FSCTL_R. Devest FSCTL_R. Thread 0: 2018 Garay Name Caray Honde Tag. Deverd Access 0. Caray Hende Tag. Deverd Access 0. Caray Hende Tag.		
Name	Event Court Event Byt	es Pending Events	Process Court Declarary Court	Ican Court Connected	
Process Haritar can stars a sambain virtual menory (in	ted by the system cannot lend, or in a file	pau spacify dented by them	dek spece), titleb de yes prefert		
O'Use virtual newsy (0,70240 available)					
Use Renamed: C. Liers/per-Schines/Desite	elprocener_pulper(best:.pel				
K					_
ProManiaad: 0.49% @pl (Siryles pending)					OK Canon
Explore D.C. 200 Charlos HCR. Explore D.C. 200 Charlos HCR. Splore D.C. 200 Charlos HCR.	Applicational vertex all anne Applicational vertex ad aver Applicational vertex ad aver	SUCCESS SUCCESS SUCCESS	Destrud Access: R Guary Name		

3. Na ferramenta Procmon, vá para **Options -> Enable Boot Logging (Opções -> Ativar registro de inicialização)**.

🎒 Pn	ocess Monit	or - C:\l	Users),win	7x64-rww\/Desktop	piprocmon_output/test1.pml				
File	Edit Event	Filter	Tools	Options Help					
l el f		E.L	- A	Alumnum	Ten I				
			Y 🗛 🤉	Adversion	rep				
Tree .	Process 7	lare .	PID	Fort			Renit	Detail	
12:36:	. IF Search	hdeer.	2252	Hablaht	alara -		SUCCESS	Cantrol: FSCTL_Q	
12.36:	. It Search	ndeser	2252				SUCCESS	Cantrol: FSCTL_R	
12:36:	. #!Search	rckeer.	2252	Configure	Symbols	1	SUCCESS	Cantral: FSCTL_R	
12.36.	<ul> <li>Search</li> </ul>	FilterHos	. 2072	erice		1	SUCCESS	Thread ID: 2884	
12:36:	- Dekow	EXE	2368	Select Colu	mna		SUCLESS	Query: Name	
12.86.	- Carpore	EVE	2968	Mater De	ath.		SUCCESS	Query: Handle Tag	
12.36:	- CERCA	EAR STREET	2300	reactly be			SUCCESS	Guery: Handle Leg	
12.36.	. Boose	EVE.	2010	Profiling Ex	anta		3000535	Desred Access: U.	
12.36	- Depart	EVE					SUCCESS	Guery: Hands Tes	
12.36	- Colore	606	2548	Envible Boo	t Logging		0000000	Centred Access M	
12.36	Deter	EXE:	2568				20200000	Ture BIG S7 In	
12.36	Enlow	DE	2568	V Show Resol	Ived Network Addresses Chi+N		SUCCESS	We need the work	
12.36	Encion	EXE	2568	Hex File Of	feets and Lengths	-	SUCCESS		
12:36	Emiore	DE	2568	H- 0	a and Thread ID-		SUCCESS	Query: Name	
12.35	Exclore	EXE	2968	Page Proces	and Thread Lin	-	SUCCESS	Query HandleTag	
12:36	Eploy	DE	2988	RegQueryKey	HKEU/Software/Classes		SUCCESS	Query: Handle Tag	
12:36:	Explore	(EXE	2968	RegOpenKey	HKEU/Software/Classes/.pnf/Open/WithProvids		NAME NOT FOUND	Desired Access: R	
12:36	Eplow	ENE	2988	RegOpenKey	HKCR\pm\OpenWithPropide	1	NAME NOT FOUND	Desired Access: R.	
12:36:	- Dekore	(EXE)	2968	RegQuer/Ker	HKCU/Software/Classes	1	SUCCESS	Query: Name	
12:36	Epion	BE SG	2968	RegiliveryKey	HKCU/Software/Cleaner	1	SUCCESS	Query: HandleTag	
12.36:	. Dokore	(DE	2968	RegQueryKey	HKCU/Software/Classes	1	SUCCESS	Query: HandleTag	
12.36:	- California	e DE	2948	RegOpenKey	HICU/Software/Classes/Software/Microsoft/We	indews\Cur1	NAME NOT FOUND	Destred Access: R.	
12.36:	. Calbolore	(DE	2968	RegOpenKey	HKCR\Software\Microsoft\Windows\CurrentVers	sion/ExploreI	NAME NOT FOUND	Desired Access: R	
12:36:	. 🎇 Epiow	DE:	2568	RegiliueryKey	HICU/Software/Classes	1	SUCCESS	Query: Name	
12.36:	<ul> <li>Bekore</li> </ul>	(DE	2968	RegQueryKey	HKCU/Software/Classes	1	SUCCESS	Query: HandleTag	
12:36:	. 🙀 Explore	1 EXE	2568	RegGueryKay	HICU/Software/Classes	1	SUCCESS	Query: HandleTag	
12.36:	<ul> <li>Epiore</li> </ul>	EVE	2968	RegOpenKey	HKEU\Software\Classes\.pnl		SUCCESS	Desired Access: R	
12:36:	- Deplore	EXE	2568	Regularyflay	HKEU/Software/Microsoft/Windows/Eurent/Vers	sion \Explore 3	SUCCESS	Query: Handle Tag	
12.36:	- Delote	EXE	2968	RegOpenikey	HKCU/Software/Morosoft/Windows/Current/Vers	son Explore	SUCCESS	Desired Access: R.	
12.36:	- Diplore	EXE	2368	Hegulueryfwy	HALU-Software Microsoft Windows Lurent Vers	sion (Explore	SUCLESS	Guery: Handle I ag	
12.86.	. apport	EAE	2998	Hegupenkey	HALU-Software unclosed invinces current vers	son Explore	50.0555	Desred Access: H.	
12.26	- Deserve	EVE	1200	Reg avery fair	Invalue Conversion of Control of	son uppere	SUCCESS	Deviced Access O	
12.36	. autom	0.00	2500	Bardumilitie	HILL C SCHWARE CHOOSEL CHINESENS SCHREIT VERS	son Explore	0000635	Time BEO 57 La	
12.36	Entire	EXE	2548	Bay Drankey	HIC'ID Schware/Microsoft/Wordson/Consect/and	sion) Funiture 1	2233310	Other canana and and	
12.36	Enlow	EVE	2568	Bag heater	HICLD Software Microsoft Windows Current Vers	story Explore	SUCCESS		
12.36	Ecity	EXE	2968	Reg Diselley	HKCU/Software/Microsoft/Windows/Current/Jers	sion' Emiliae 1	SUCCESS		
12:36	Estore	DE	2988	Requester	HKCU/Software/Classes		SUCCESS	Query: Name	
12:36:	Epplore	EXE	2968	RegQuenKey	HKEU/Software/Classes		SUCCESS	Query HandleTag	
12:36:	Epilore	EVE:	2988	RegQueryKey	HKEU/Software/Classes	-	SUCCESS	Query: Handle Tag	
12:36:	. EDplore	(EXE)	2968	RegOpenKey	HKCU/Software/Classes'Applications'instead e	sie 1	NAME NOT FOUND	Desired Access: R.,	
12:36	Eplow	DE	2968	RegOpenKey	HKCR\Applications\notepad are	1	SUCCESS	Desired Access: R.	
12:36:	- Dekore	(DE	2968	RegDoseKey	HKCR'Applications'unstepad eve	1	SUCCESS		
12:36:	- Epilore	B/E	2968	RegiouryKey	HKCU/Software/Cleases	1	SUCCESS.	Query: Name	
12.36:	- Dekore	(EXE)	2968	RegQueryKey	HKCU/Software/Classes	1	SUCCESS	Query: HandleTag	
12:36:	- 🙀 Epian	DE	2968	RegiliueryKey	HREU/Software/Classes		SUCCESS	Query: HandleTag	
12.36:	- Bekore	(DE	2968	RegOpenKey	HRCU-Software/Classes'Applications'instepad e	540 1	NAME NOT FOUND	Desired Access: R.,	
12:36:	- Epice	EXE	2568	RegOpenKay	HRCRVApplications Vrotepad ase	1	SUCCESS	Dealred Access: R.	
12.36:	- Bokore	EXE	2968	RegQueryRey	HRCR Applications instepad eve		SUCCESS	Query: Name	
12:36:	- pplan	EXE	2368	fleg Juery flay	MALH Veptications Viotepad ase		SUCCESS	Query: Handle Tag	
12.16	A DECK OF	a la	7960	AND DODO DO	and the second sec	and the state of the	NAME AND AND AND	second access D	

4. Selecione Gerar perfis de ameaças e a cada segundo.

🎒 Proc	ess Monitor - C:\	Users\win7x64-new\Desktop	p/procmon_output/test1.pm	1			
File Ed	St Event Filte	r Tools Options Help					
i 🔤 🔚	🔍 🖉 🕼	🏹 🛆 영어 🔟 🛤 🧃					
Time	Process Name	PID Operation	Path		Result	Detail	
12-16-	Caarthindexer	2252 KieSustenContra	10-		SUCCESS	Control: ESCTL Q	
12:36	Searchindexer	2252 FileSystemContro	IC:		SUCCESS	Control: ESCTL_R	
12:36	19/10/10			0	SUCCESS	Control: ESCTL_R	
12:36	Enable Boo	xt Logging			SUCCESS	Thread ID: 2884	
12:36	E				SUCCESS	Query: Name	
12:36	Process Mo	onitor can generate thread pro	fling events that capture		SUCCESS	Query HandeTag	
12:36	The scace of	or all running applications at a r	eguar interval.		SUCCESS	Query: Handle Tag	
12:36	E Gen	erate thread profiling events			SUCCESS	Desired Access: Q	
12:36	E				SUCCESS	Query: Name	
12:36	6	Every second			SUCCESS	Query: Handle Tag	
12:36	E	C Every 100 millioncoods			SUCCESS	Desired Access: M	
12:36	E	C creft and managements		(Default)	SUCCESS	Type: REG_SZ, Le	
12:36	6		OK Cancel		SUCCESS	-	
12:36	E	_			SUCCESS		
12:36	Explorer.EXE	2988 KRegQueryKey	HKCU/California/Classes		SUCCESS	Query: Name	
12:36	Explorer EXE	2988 RegQueryKey	HKCU Software Wasses		SUCCESS	Query: Handle Tag	
12:36	Explorer EXE	2988 RegQueryKey	HKCU/Software/Classe		SUCCESS	Query: Handle Tag	
12:36	Explorer.EXE	2988 KRegOpenKey	HKCU/Software/Classes/.pml/	OpenWithProgids	NAME NOT FOUR	ND Desired Access: R	
12:36	Eplow-EXE	2988 RegOpenKey	HKCR\pml\OpenWithProgids		NAME NOT FOUR	ND Desired Access: R	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name	
12:36	Explorer.EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: HandleTag	
12:36	Eplorer EXE	2988 KRepQueryKey	HKCU/Software/Classes		SUCCESS	Query: HandleTag	
12:36	Explorer.EXE	2988 KegOpenKey	HKCU/Software/Classes/Softw	<pre>ware\Microsoft\Windows\Curr</pre>	NAME NOT FOUR	ND Desired Access: R	
12:36	Explorer.EXE	2988 KRegOpenKey	HKCR\Software\Microsoft\Wv	ndows\CurrentVersion\Explore.	NAME NOT FOUR	ND Desired Access: R	
12:36	Explorer EXE	2988 KRepQueryKey	HKCU\Software\Classes		SUCCESS	Query: Name	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU/Software/Classes		SUCCESS	Query: HandleTag	
12:36:	Explorer.EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: HandleTag	
12:36	Explorer EXE	2988 KegOpenKey	HKCU\Software\Classes\.pml		SUCCESS	Desired Access: R	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Mcrosoft\W/	>dows\CurrentVersion\Explore.	SUCCESS	Query: HandleTag	
12:36:	Explorer.EXE	2988 KRegOpenKey	HKCU\Software\Mcrosoft\Wv	ndows/Current/Version/Explore.	SUCCESS	Desired Access: R	
12:36	Eplorer.EXE	2988 KRegQueryKey	HKCU/Software/Microsoft/Wir	ndows/Current/Version/Explore.	SUCCESS	Query: Handle Tag	
12:36	Explorer EXE	2988 KRegOpenKey	HKCU\Software\Mcrosoft\W/	<pre>&gt;dows\CurrentVersion\Explore.</pre>	SUCCESS	Desired Access: R	
12:36:	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Microsoft\W/	ndows/Current/Version/Explore.	SUCCESS	Query: HandleTag	
12:36	Explorer EXE	2988 KegOpenKey	HKCU\Software\Mcrosoft\Wr	ndows \Current Version \Explore.	SUCCESS	Desired Access: Q	
12:36	Explorer EXE	2368 RegQueryValue	HRCU/Software/Microsoft/W/	dows \Current Version \Explore.	SUCCESS	Type: REG_SZ, Le	
12:36	Explorer EXE	2908 RegCoseKey	HRCU/Software/Microsoft/W/	ndows \Current Version \Explore.	SUCCESS		
12:36	Diplorer EXE	2368 RegCoseKey	HRLU Software Microsoft Wir	ndows \Current Version \Explore.	SUCCESS		
12.36	Explorer EXE	2368 RegCloseKey	HRLU/Software/Mcrosoft/W/	ndows \Current Version \Explore.	SUCCESS		
12:36	Explorer EXE	2308 RegQueryKey	HRCU/Software/Classes		SUCCESS	Query: Name	
12:36	Diplorer EXE	2968 KegQueryKey	HRCU Software Classes		SUCCESS	Query: Handle Tag	

5. Verifique se todos os filtros relevantes estão selecionados em Procmon e se os dados estão sendo coletados.

6. Se você não conseguir replicar o travamento, você pode forçar o travamento do Windows usando o utilitário NotMyFault64.exe que você pode obter do <u>https://live.sysinternals.com/files/</u>

As instruções sobre como executar estão aqui: <u>https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump</u>

A CRE CARE FROM	North Options Pade				
8 B 3 8 6 7	40 2 4 4				
in . Prosting	ND deeper	Fut.	fault .	Ganal	
the Windows	THE BARAN	Company Resident AMP 211 Marcen by	9.00201	Other Distances	
18. B Marco	100 Castrings	C Program Res Carol (MP1111) FLow Inc.	9.00200	Ware Center Te.	
138 - W Marco	1707 Charly Winfords	C Vegen RenCennel#13114Lawing	8,0101-040701	Department 161	
13. K.M. en	170 Charles Tex	18,54 Selware Human Western VC creet/assors for	NUMBER	ODent Arrest R.	
28. B.M.m.	The second second	HEM Schware Human Western VF Current Innor Tre	NAME AND POST	COunt Arrest 5.	
28. E.M. 40	The Courter for	HEM Selvery Hunsel' Medine 17 Cyter/lenser Str.	NOT YOUR	Control Access P.	
1	The party and a start	Constant and and an end of the set of	100.000	Accession (Sec.	
	The second second	Conception of the case of the second se	100.000	State of the local	
	The second second	Contraction of the second seco	The second second	When when he	
1	The Day Minholes	F Changer Services diff. 11 ft di ser ba	a press lupper	Canadian Trans. 1-54	
The Party of Lot	110 Charlester	18 M Schwarz Hotself Westwork? Complement for	said out them	Constant Access 10	
H. Kittan	100 Charles have been been been been been been been be	18, M Schwarz Hutself Ministree MP Current lesson file.	NAME AND POST OF	COMPACT ACCESS 19	
<ol><li>Element</li></ol>	The Construction	18,14 Selven Hoted' Medine 17 Catentieson Inc.	AND NOT YORK	COMMENCED IN	
3. Ext.ee	170 Bolandarded.	Proper Nerri accular 1114 de las las	140.005	Access for 2.	
S. 19140	The Banchardert	Proper Nerrosci 48" 1114" de la	100.000	Accession (R.).	
3. EV. 44	The second second	Proper Nerces and Think are by	1.41.211	the post of	
	The subscription of the su	And the second second second second	10.00	Contraction in the	
	in the second	THE R. LANSING MICH.	south said of	And and Address of the	
	I INC. Manual Insuition	out of Schwarz Schwarz Western W. L. continuers in	NAME AND ADDRESS.	And in case of the local division of the	
in Electrony	1 IN CONTRACTOR	The M Schwarz (Restard) Ministers 10" Contentionness for	NAME OF TAXABLE	Column Array in	
in Eldines	100 Alanchanast	E Vropen RenCentral#1015 et als rentes	9.00 (1995)	Accession (A.	
<ol> <li>Extent</li> </ol>	100 Milandarowit	Company Rendershall Publishers and In-	9,00,000	Acception in	
<ol> <li>Evene</li> </ol>	THE BURNING	( Proper Net (act 44* ) 15 4t eve to	9.40.005	Mag 25 (91) (10)	
<ol> <li>Extent</li> </ol>	THE DUNCTION	Proper NerCent AP Indon B	940,995	Dolane half.	
E. 10.44	THE REAL PROPERTY.	The second second second	B.41.895	Deliana Pasa ()	i interative Citikedentiliper (2) yealaan
	in another	Proper Nerces AP 1404.8	PAR PRO	1004105003	Evaluation and applied states
	The second second	Constant and the case of the second	And the second second	COMPANY ACCOUNTY,	Contraction of the International Actions in the International Actional Actional Actional Actional Actio
	and the second	Comparison and the state of	The second second	and in long-	Contraction of Section 2010
	in a landariat	Comparing the case of the second	5.00 Mpt	Sector 1	Excellence of the first difference of the other part of the first section of the first sec
	The second state	Company Review of Street, do	0.41 000	Other Laboration	The second
1.	110 Bulgarintenan	Company Republican (1971) 11 Hot results	0.00000	where a story in	WEIGHT STATUS WARRY OF THE TOP
C. B. Marrie	110 Bullan Minteres	Company Revolution (1997) 11 High rate (19	8. Philip July 1	Castor Ing. 14	3 January of Continentwool/Mddmeendedimap
<ol> <li>Element</li> </ol>	110 Paginettes	HLM School Hensell Western M Carentiesers Inc.	NAME AND POST	Classed Access PL	an and data at the set of the set of the set
<ol> <li>Element</li> </ol>	110 Paginetter	HKM Schwart Hensell Westwart Tr Caractilasers Ter.	NUMPROFILE	Classe Arrest R.	ACCRETE TO ALL PROPERTY AND ADDRESS OF ADDRESS
<ol> <li>Extension</li> </ol>	110 Pagitorito	HEAV Schwarz (Renault Westers) 11 Caractilators (In-	NUMEROF FORM	Of Autorit Access 14.	B 45 (B) 10 (C B) (C B) (C B) (C B)
<ol> <li>E. E. M. and</li> </ol>	110 Australia	C Vergeen Ren Carol all P (151) at use by	0.40.0005	Restorder 2.	and other states and s
8. EX. 44	110 Million Nantari	C Vegen Rel Cechild* 1111 at see by	9.40.995	Rented as A	Trinset Number of the latent
	IN A REAL PROPERTY OF	Contraction and Contraction of the second	The second second	the states.	3 Digrini 20, 875, 686, 751 Autor Area
	The second second	Company Network and Company and State	A COMPANY OF THE OWNER.	Contraction 14	the discovery and that it may discriminate for the discovery holds in a
0.002	10 That series	of M Information of Manager M Complement In-	same and shares	Contract Income 18	
2 P. 2 C	110 Charlester	with M. Schwarz Stream of Minimum VP Complement Ten	said of the	Contrast Acress 10	Producer in a local device operating of an example of a local state of
N. Kithan	110 Paul Inches	HEAV School (Renaul) Western W Compliance Inc.	water white where	Contrast Arrange 4	
10. B Marcol	100 allow having	C Proper RenCent (MP-11) Returns to:	9.40399	Avairily 3.	Epsteen valahid mandaditapolaria tanan dalah angkal tidan sa mangan ja zona.
<ol> <li>E. Marson</li> </ol>	100 Mancharderi	2 Proper Re/Cas/JMP/118 down he	9.00595	Rentring 3.	
<ol> <li>Elden</li> </ol>	100 Million fee	C Propert RenCent AMP/2018 at case ba	9.00895	One 2018-625	
	N Alastrianate	2 Proper Ner Carrister (201 at sec by	PALET	warmington In.	1
	In anything	<ul> <li>Prepare Net Card AMP (11) &amp; drawing</li> </ul>	A PROPERTY.	Coatter Tree 1-5	1
	The second second	the of the second strates of coversions in	And April 1044	And Access in	1
	The second second	of the second decade of the second se	And the state	Contract Across 1	1
	100 milesterio	Colorano Residenci dell'ALE di una lor	B-CORD	decate line 12	1
a di di ana	100 Alambarian	C Western Res Claire and Clair and Annual In-	B-CODIN	Rentring 3	(
<ol> <li>B Manuel</li> </ol>	100 Advin	C Property Res Carlot (1997) 21 R efficiencies	0.00000	Ofer 25,000,011	1
<ol> <li>B Muse</li> </ol>	100 Campionate	C Property Res Card (007-11) R all use her	PLOCENT.	Ware Center Te.	1
<ol> <li>B Mines</li> </ol>	100 Casherine	C Propert RenCatal AMP/2018 All and her	BUTTER DISTANCE	Date Tra 16	1
<ol> <li>E Manuel</li> </ol>	100 Charles for	HEM Scheme Honsell Window M Constitution Tox	NUMEROF POINT	O'Dent Arrest R.	1
	The Conference	HEM Select Honey Write M Contributor Str.	AND REPORT ADAM	COntrol Arrises PL	1
	The Production	HEAP Scheme (Roman) Windows 10" Current Server Street	NOT YORK	Control Acres P.	\ \
	W Carlenbergelt	C Prepare Ren Caron aller 15 II all une ha	PLOCEN	Accession 2.	
	The Date Spring	- Property rest Card All - 1 - 1 - 41 and by	PLACE IN	Manager Day 28.	
and the second second	The second se	Company of Card and Card and Annual State	PARTY OF THE OWNER	Contract in the local division of the	
	THE PROPERTY.	THE R. LEWIS CO., LANSING MICH.	B. COMP.	Same Reads in	
a second second	THE PARTY CONTINUES.	NEW STREET, MARKING MICH.	8.0000	Castral Array 1	
a sugar an	THE Property	NEW SCHOOL BOARD ADDIVINES	0.0000	Grave N.S. Subme	
Compression and	200 Children Burt	NEW SOFTWARE ASSAULT ADDIVIDUO	BUTTEN TOO THE		
Compression and	COD Conclusion	NUMBER OF ANY ADDRESS OF ADDRESS OF	9.0.00	Tax FELSE in	
C. B. Marrie and	200 Challen	HEM SOFTWARE ASSAULT ADDIVIDUAL	PLOCEN		
<ul> <li>A sequence are</li> </ul>	200 Children Per	HE N	PLOCEN	Dary Ambridg	
<ul> <li>A service are</li> </ul>	200 Challenter	HEAD OF TAME Association (MERCAN)	PLOCEN	Chanal Access 10	
1. B 100000.000	CRI Challenge	NUMBER OF STREET ACCOUNTS AND ADDREED ADDR	PLOCEN:	Gary N.K. Sality	
A	CRI Charlenger	NUMBER OF THE ADDRESS OF THE OWNER	\$0770 NO. 54	A	
and the second se		THE R. P. LEWIS CO., NAME AND ADDRESS OF TAXABLE PARTY.	PLATE COL	THE PERSON IN	
a subset	Contraction of the second second	and he shall be all a set of a state of the set of	the selected second		

7. Quebre a máquina.

8. Inicialize a máquina no modo de segurança e colete manualmente **Procmon.pmb** e **MEMORY.DMP**, ambos os arquivos estão em C:\Windows folder. Esses arquivos devem ser compartilhados com o Cisco TAC.

🗼 Windows					_	8
🕞 🕞 🖉 🗸 Computer	r 🕶 Local Disk (C:) 💌 Win	dows 👻	÷ 🔯	Search Windows		
Organize 👻 🗋 Open 💌	New folder				)III • 🚺	
🚖 Favorites	Name +		Date modified 11/21/2010 4:24 AM	Type Application	Size 2,805 KB	
<ul> <li>□ Libraries</li> <li>□ Documents</li> <li>□ Music</li> <li>□ Pictures</li> <li>□ Videos</li> </ul>	<ul> <li>fveupdate.exe</li> <li>HelpPane.exe</li> <li>hh.exe</li> <li>IE11_main.log</li> <li>MEMORY.DMP</li> <li>mib.bin</li> </ul>		7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/6/2020 12:41 PM 7/14/2009 1:06 AM	Application Application Application Text Document DMP File BIN File	15 KB 717 KB 17 KB 14 KB 331,914 KB 43 KB	
P Computer Cocal Disk (C:) CD Drive (D:) Shared Folders (\\vn	<ul> <li>msdfmap.ini</li> <li>notepad.exe</li> <li>ntbtlog.txt</li> <li>PFRO.log</li> </ul>		6/10/2009 10:36 PM 7/9/2015 7:57 PM 1/6/2020 12:41 PM 1/6/2020 12:30 PM	Configuration sett Application Text Document Text Document	2 KB 189 KB 83 KB 576 KB	
📭 Network	ProcessionalN.xml ProfessionalN.xml Professional	Type: XML Document Size: 52.3 KB Date modified: 6/10/20	1/6/2020 12:41 PM 6/10/2009 10:30 PM 2:39 AM 2:30 PM 2:30 PM 2:30 PM 1/14/2009 0:56 AM 11/21/2010 4:24 AM 6/10/2009 10:31 PM	PMB File XML Document Application Text Document Text Document Application XML Document	320,740 KB 53 KB 417 KB 29 KB 0 KB 66 KB 48 KB	
Procmon.pmb PMB File	Date modified: 1/6/2020 1 Size: 313 MB	2:41 PM Date crea	ated: 1/6/2020 12:41 PN	И		

7. Opcionalmente, se você puder inicializá-lo no "modo normal" se os arquivos PMB forem gerados no diretório C:\Windows folder, se você iniciar o ProcMon novamente, verá os seguintes registros. A partir disso, você pode salvar novamente os eventos clicando no botão Salvar.

Precess Monitor - Sysintemais: www.sysintemais.com			
File Edit Event Filter Tools Options Help			
2 2 3 5 5 7 4 4 1 A 4 8 2 3 4 5			
Tour Pourse Name FD Damaian, Faih	Read	Detel	

Pasara Munitor	Ξ
2 log of loost time unitaly says control by a persistal indexes of Process Meetins. On you with in solve the collected data wou?	
Tes	
/	
/	

_
Genet

🔰 Process Monitor - Sysi	internals: www.sysinternals.	com		
File Edit Event Filter	Tools Options Help			
📽 🖬 🔌 🕸 🖾 🛛	⇒ <b>∆</b> ⊕ 🖲 🖊 🖣			
Time Process Name	PID Operation	Path	Result	Detail
12:41: Fames exe	292 🧟 Process Start		SUCCESS	Parent PID: 4, Com
2.41: Famas exe	292 ar Thread Create		SUCCESS	Thread ID: 295
2.41: Tames exe	292 E Load Image	C:\Windows\System32\amss.exe	SUCCESS	Image Base: 0x479
2.41: Pamas exe	292 ar Load Image	C:\Windows\System32vitdl.dll	SUCCESS	Image Base: 0x779
241: Pamas exe	292 RegOpenKey	HKLM\Software\Morosoft\Windows NT\CurrentVersion\Ima	NAME NOT FOUN	D Desired Access: Q
41: Fames exe	292 RepOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R
2.41: Pamas exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41 smss.exe	292 KRegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 1.024
41: E smss.exe	292 KRepQueryValue	HKLM'\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 1,024
41 smss.exe	292 RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	
41: Pamas exe	292 Koreate File	C://Windows	SUCCESS	Desired Access: E
41 Smss.exe	292 ReadFile	C:\\Windows\System32\amas.exe	SUCCESS	Offset: 74,752, Len
41: Pamas exe	292 🛃 ReadFile	C:\Windows\System32\amss.exe	SUCCESS	Offset: 1,024, Long
41 Smss.exe	292 ReadFile	C:\Windows\System32\amsa.exe	SUCCESS	Offset: 107,008, Le
41: Resmos.exe	292 MeadFie	C:\Windows\System32\amas.exe	SUCCESS	Offset: 104,448, Le
41 smss.exe	292 See Thread Create		SUCCESS	Thread ID: 300
41: Romas exe	292 ReadFile	C:\Windows\System32\amas.exe	SUCCESS	Offse Offset: 104,448
41 smss.exe	292 KeadFile	C:\Windows\System32\amsa.exe	SUCCESS	Offse Length: 2,560
41: Ersmas exe	292 KegOpenKey	HKLM'\System\CurrentControlSet\Control\MinINT	REPARSE	Desi L/O Rags: Non-cached, Paging L/O, Synchronous Paging L/O
41: Famos exe	292 RegOpenKey	HKLM\System\CurrentControlSet\Control\MnINT	NAME NOT FOUN	D Desi Priority: Normal
41: Pamas exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\.	REPARSE	Desired Access: Al
41: I smss.exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\.	SUCCESS	Desired Access: Al
41: Pamas exe	292 KRegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	0
41: Pamos exe	292 RepSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_SZ, Le
41: Pamas exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R
41: I amos exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41: Famas exe	292 KRepQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_DWO
41: Internet exe	292 RegQueryValue	HKLM'System'CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_MULT
41: Stres exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_MULT
41: Elamos exe	292 RegQueryValue	HKLM'System'CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_MULT
41 Stres exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 4,094
41: Elamos exe	292 RegQueryValue	HKLM'System/CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_DWO
41: Smiss.exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	D Length: 4,094
41: emes.exe	232 RegQueryValue	HKLM System/CurrentControlSet/Control/SESSION MANA	NAME NOT FOUN	D Length: 4,094
41 Smiss.exe	232 ReguleryValue	HKLM System CurrentControlSet Control SESSION MANA.	NAME NOT FOUN	D Length: 4,094
41: erismes.exe	232 ReguleryValue	HKLM System CurrentControlSet Control SESSION MANA.	SUCCESS	Type: NEG_MULT
41. Smiss.exe	252 RegOpenkey	HKLM System CurrentControlSet Control SESSION MANA.	SUCCESS	Desred Access: M
41:	202 Preguleyvaue	HKLM System Current Control SESSION MANA.	SUCCESS	Type: NEG_MULT
41 amos exe	252 Reguleyvaue	HKLM (System CurrentControlSet Control (SESSION MANA	NAME NOT FOUN	U Length: 4,094
41 Promosieve	202 Preguleyvaue	HKLM System Current on the Control SESSION MANA.	50006555	Type: HEG_HOLT
41 Smos.exe	252 Repuese value	HKLM (System CurrentControlSet Control (SESSION MANA	SUCCESS	
41	202 Preguoseney	HALM System Current on book Control SESSION MANA.	2000622	Desired Assess M
41	202 Reguperkey	INCH Gyster Correct Control State Control SESSION MANA.	CUCCESS	Index O Name A
A1 Brance and	202 PasEn militar	LVI M Custon Custon Custon Caston Control COCCOM MANA	CINCESS	Index 5 Name M
41	292 RecEnceValue	HALM CYREM LUTERLOTED SELLOTED SELLOTED SESSION MANA	SUCCESS	Index 3 Name M
A1 Brends and	292 ResEnceValue	LVI M Crater Crater Control Set Control SESSION MANA	CLUCEDO	Index 3 Name Of
di amos exe	202 Regenunivaue	HALM Gyster Lutter Lore Dist Lore Disc 53504 MANA.	CUCCESS	Index 4 Name 8
A1 Press eve	292 ResEnceValue	LIVE ME System Control Set Control SESSION MANA	0000633	Index 5 Name 11
41	202 Progenum value	HALM Gyster LUTERLOTED SR. LOTED SESSION MANA.	NO MODE ENTER	Index: 6 Lanoth: 4
A1 Brance and	292 Regenuit value	HALM System Control Set Control SESSION MANA.	SUCCESS	
41	292 ResOurceMay	HIGH Grand Control Control Control CERCICAL MARKA	CUCCESS	Daried Access M
supercise	eve meguperney	INTER OVER COLORDON FORD SE22YON WARK.	3000633	VEHEV /VVEH. P